(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 1 519 509 A3**

(12) **EUROPEAN PATENT APPLICATION**

(88) Date of publication A3:
21.03.2007 Bulletin 2007/12

(43) Date of publication A2:
30.03.2005 Bulletin 2005/13

(21) Application number: **04255950.0**

(22) Date of filing: **29.09.2004**

(51) Int Cl.:
H04L 9/06 *(2006.01)*

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LI LU MC NL PL PT RO SE SI SK TR
Designated Extension States:
AL HR LT LV MK

(30) Priority: **15.03.2004 US 800983**
29.09.2003 US 507004 P

(71) Applicant: **VIA Technologies, Inc.**
Taipei 231,
Taiwan (TW)

(72) Inventors:
- **Henry, G. Glenn**
  Austin
  Texas 78746 (US)
- **Crispin, Thomas A.**
  Austin
  Texas 78738-5015 (US)
- **Parks, Terry**
  Austin
  Texas 78737 (US)

(74) Representative: **O'Connell, David Christopher**
HASELTINE LAKE,
Redcliff Quay
120 Redcliff Street
Bristol BS1 6HU (GB)

(54) Apparatus and method for providing user-generated key schedule in a microprocessor cryptographic engine

(57) The present invention provides an apparatus and method for performing cryptographic operations on a plurality of input data blocks within a processor. In one embodiment, an apparatus for performing cryptographic operations is provided. The apparatus includes a cryptographic instruction, keygen logic, and execution logic. The cryptographic instruction is received by a computing device as part of an instruction flow executing on the computing device. The cryptographic instruction prescribes one of the cryptographic operations, and also prescribes that a user-generated key schedule be employed when executing the one of the cryptographic operations. The keygen logic is operatively coupled to the cryptographic instruction. The keygen logic directs the computing device to load the user-generated key schedule. The execution logic is operatively coupled to the keygen logic. The execution logic employs the user-generated key schedule to execute the one of the cryptographic operations.

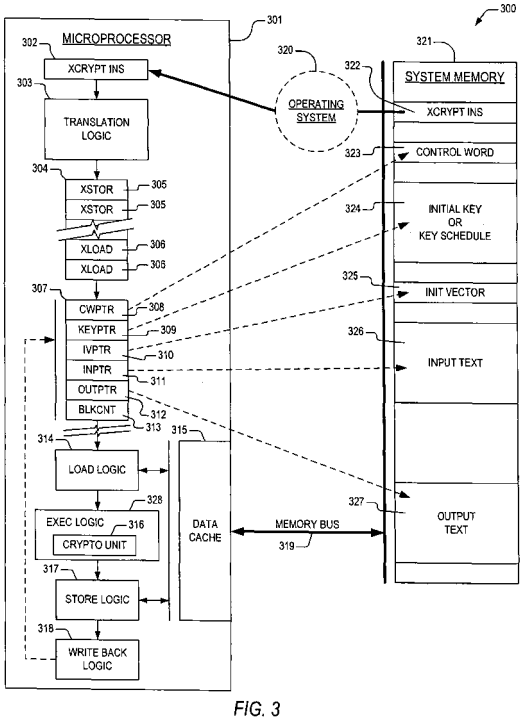

FIG. 3

Printed by Jouve, 75001 PARIS (FR)

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 04 25 5950

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	WO 01/17152 A (COPPE UFRJ COORDENACAO DOS PRO [BR]; CARDOSO SALOMAO SERGIO LUIZ [BR];) 8 March 2001 (2001-03-08) * abstract * * page 1, line 1 - line 10 * * page 7, line 24 * * figures 3,4 * -----	1-3,5-8, 10,12	INV. H04L9/06
A	EP 1 215 842 A (BROADCOM CORP [US]) 19 June 2002 (2002-06-19) * abstract * * paragraph [0001] - paragraph [0011] * * paragraph [0022] - paragraph [0023] * * paragraph [0030] - paragraph [0044] * * figures 4a,4b * -----	1-13	
			TECHNICAL FIELDS SEARCHED (IPC)
			H04L

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
The Hague	12 February 2007	Liebhardt, Ingo

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

1

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 04 25 5950

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

12-02-2007

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0117152 A	08-03-2001	AU 6072599 A	26-03-2001
		BR 9903609 A	24-04-2001
EP 1215842 A	19-06-2002	US 2002108048 A1	08-08-2002

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82